



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

50

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/916,981	07/26/2001	Igor G. Mutik	NAIIP018/01.095.01	8531
28875	7590	04/26/2005	EXAMINER	
Zilka-Kotab, PC P.O. BOX 721120 SAN JOSE, CA 95172-1120			POPHAM, JEFFREY D	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 04/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/916,981

Applicant(s)

MUTTIK, I. ET AL.

Examiner

Jeffrey D. Popham

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 March 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3, 6-17 and 20-33 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 31-33 is/are allowed.
- 6) ☒ Claim(s) 1-3, 6-8, 13-22 and 27-30 is/are rejected.
- 7) ☒ Claim(s) 9-12 and 23-26 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 July 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Remarks

Claims 1-3, 6-17, and 20-33 are pending.

Claim Objections

1. Claim 29 is objected to under 37 CFR 1.75(a) because of the following informalities:

- Claim 29, line 12 recites the limitation "the server". There is insufficient antecedent basis for this limitation in the claim. For purposes of prior art rejection, it has been construed as "a server".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

1. Claims 1, 3, 6-8, 13-15, 17, 20-22, and 27-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hypponen et al. (U.S. Patent 6,577,920) in view of Vibert (Vibert, R., "A Day in the Life of an Anti-Virus Lab", 6/17/2000, pp. 1-5, obtained from <http://www.security-focus.com/infocus/1268>).

Regarding Claim 1,

Hypponen et al. disclose a method for detecting viruses in software, comprising:

(a) comparing subject data with a plurality of virus definitions in a first database (Column 4, lines 60-67; and Column 5, lines 32-41);

(b) executing a security event if the subject data is successfully compared with at least one of the virus definitions (Column 5, lines 32-41);

(c) comparing the subject data with fingerprints of innocent data in a second database [combination of second and third databases] (Column 5, lines 42-56);

(d) allowing access to the subject data if the subject data is successfully compared to the fingerprints of innocent data (Column 5, lines 56-58); and

(e) transmitting information to a server for analysis purposes if the subject data is unsuccessfully compared to the virus definitions and the fingerprints of innocent data (Column 5, lines 58-65);

wherein the information transmitted to the server includes at least one of the subject data and a fingerprint associated with the subject data (Column 5, lines 58-65, referring to transmitting the subject data).

Hypponen et al. do not disclose that the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent.

Vibert, however, discloses that the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent (Page 1, Paragraph 4 through Page 2, Paragraph 1). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the virus lab of Vibert into the virus screening system of Hypponen et al. in order to provide a means for consistently detecting new viruses without triggering any false alarms on otherwise innocent files (Page 3, Paragraph 3).

Regarding Claim 15,

Claim 15 is a computer program product claim that corresponds to method claim 1 and is rejected for the same reasons.

Regarding Claim 29,

Claim 29 is a system claim that corresponds to method claim 1 and is rejected for the same reasons.

Regarding Claim 3,

Hypponen et al. discloses reporting that the subject data is innocent if the subject data is successfully compared to the fingerprints of innocent data (Column 5, lines 53-58).

Regarding Claim 17,

Claim 17 is a computer program product claim that corresponds to method claim 3 and is rejected for the same reasons.

Regarding Claim 6,

Vibert discloses comparing the fingerprint associated with the subject data and fingerprints associated with innocent data in a third database at the server (Page 1, Paragraph 4).

Regarding Claim 20,

Claim 20 is a computer program product claim that corresponds to method claim 6 and is rejected for the same reasons.

Regarding Claim 7,

Vibert discloses comparing the fingerprint associated with the subject data and fingerprints associated with virus definitions in a fourth database at the server (Page 2, Paragraph 1).

Regarding Claim 21,

Claim 21 is a computer program product claim that corresponds to method claim 7 and is rejected for the same reasons.

Regarding Claim 8,

Vibert discloses that the third and fourth databases are updated more frequently than the first and second databases (Page 4, Paragraph 1).

Regarding Claim 22,

Claim 22 is a computer program product claim that corresponds to method claim 8 and is rejected for the same reasons.

Regarding Claim 13,

Vibert discloses that the information is transmitted to the server via the Internet (Page 4, Paragraph 3).

Regarding Claim 27,

Claim 27 is a computer program product claim that corresponds to method claim 13 and is rejected for the same reasons.

Regarding Claim 14,

Hypponen et al. disclose that the first database and the second database are both components of a client computer coupled to the server via a network (Column 4, lines 19-22).

Regarding Claim 28,

Claim 28 is a computer program product claim that corresponds to method claim 14 and is rejected for the same reasons.

Regarding Claim 30,

Hypponen et al. disclose a method for detecting viruses in software, comprising:

- (a) comparing subject data with a plurality of virus definitions in a first database (Column 4, lines 60-67; and Column 5, lines 32-41);
- (b) executing a security event if the subject data is successfully compared with at least one of the virus definitions (Column 5, lines 32-41);
- (c) comparing the subject data with fingerprints of innocent data in a second database (Column 5, lines 42-56);

(d) reporting that the subject data is innocent if the subject data is successfully compared to the fingerprints of innocent data (Column 5, lines 53-58); and

(e) transmitting the subject data over a network for analysis purposes if the subject data is unsuccessfully compared to the virus definitions and the fingerprints of innocent data (Column 5, lines 58-65);

Hypponen et al. do not disclose that the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent.

Vibert, however, discloses that the analysis utilizes a virus detection algorithm to detect whether the subject data is malicious or innocent (Page 1, Paragraph 4 through Page 2, Paragraph 1). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the virus lab of Vibert into the virus screening system of Hypponen et al. in order to provide a means for consistently detecting new viruses without triggering any false alarms on otherwise innocent files (Page 3, Paragraph 3).

2. Claims 2 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hypponen et al. in view of Vibert, further in view of Tarbotton et al. (U.S. Patent Application Publication 2002/0,116,542).

Regarding Claim 2,

Hypponen et al. as modified by Vibert does not disclose that the security event is selected from the group consisting of cleaning the subject data, quarantining the subject data, and blocking the subject data.

Tarbotton et al., however, disclose that the security event is selected from the group consisting of cleaning the subject data, quarantining the subject data, and blocking the subject data (Page 2, Paragraph 30). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the virus removal system of Tarbotton et al. into the virus screening system of Hypponen et al. as modified by Vibert in order to provide a static warning that a previously infected file may have suffered irreparable damage so that the user of the file will be sufficiently notified of this fact (Page 2, Paragraph 31).

Regarding Claim 16,

Claim 16 is a computer program product claim that corresponds to method claim 2 and is rejected for the same reasons.

Allowable Subject Matter

3. Claims 9-12 and 23-26 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

4. Claims 31-33 are allowed because the closest prior art fails to disclose that the server requests the subject data from the client computer upon an unsuccessful comparison of the fingerprint associated with the subject data.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571)-272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER